(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2005 (15.09.2005)

PCT

(10) International Publication Number
WO 2005/086412 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/KR2005/000615

(22) International Filing Date: 4 March 2005 (04.03.2005)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:

10-2004-0015162	5 March 2004 (05.03.2004)	KR
10-2004-0046756	22 June 2004 (22.06.2004)	KR
10-2004-0098527	29 November 2004 (29.11.2004)	KR

(71) Applicants *(for all designated States except US)*: **Electronics and Telecommunications Research Institute** [KR/KR]; 161, Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR). **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR). **KT Corporation** [KR/KR]; 206, Jungja-dong, Bundang-gu, Seongnam-city, Kyeonggi-do 463-711 (KR). **SK Telecom Co., Ltd.** [KR/KR]; 99, Seorin-dong, Jongro-gu, Seoul 110-110 (KR). **KTFREETEL CO., LTD.** [KR/KR]; 890-20, Dacchi-dong, Gangnam-gu, Seoul 135-280 (KR). **HANARO TELECOM, INC.** [KR/KR]; Shindongah Fire & Marine, Insurance Building 43, Taepyeongno 2-ga, Jung-gu, Seoul 100-733 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHO, Seokheon** [KR/KR]; 775-21, Shin-dong, Iksan-city, Jeollabuk-do 570-976 (KR). **CHANG, Sung-Cheol** [KR/KR]; Expo Apt. 106-205, Jeonmin-dong, Yuseong-gu, Daejeon-city 305-390 (KR). **YOON, Chul-Sik** [KR/KR]; Seonkyeong Apt. 4-402, 255-1, Hagye-dong, Nowon-gu, Seoul 139-230 (KR).

(74) Agent: **YOU ME PATENT AND LAW FIRM**: Seolim Bldg., 649-10, Yoksam-dong, Kangnam-ku, Seoul 135-080 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2005/086412 A1

(54) Title: METHOD FOR MANAGING TRAFFIC ENCRYPTION KEY IN WIRELESS PORTABLE INTERNET SYSTEM AND PROTOCOL CONFIGURATION METHOD THEREOF, AND OPERATION METHOD OF TRAFFIC ENCRYPTION KEY STATE MACHINE IN SUBSCRIBER STATION

(57) Abstract: Disclosed is a traffic encryption key (TEK) management method for automatically generating a TEK for a multicast or broadcast service by a base station to periodically update a TEK used by a subscriber station. The base station transmits the first Key Update Command message for updating a group key encryption key (GKEK) for encrypting the TEK and the second Key Update Command message for updating the TEK to the subscriber station to update the TEK. The base station establishes an M & B TEK Grace Time which is different from a TEK Grace Time established by the subscriber station, transmits the first message including a new GKEK to the subscriber station through a primary management connection before the M & B TEK Grace Time, and transmits the second message including a new TEK encrypted with the new GKEK thereto through a broadcast connection after the M & B TEK Grace Time.